



SISTEM OPERASI KALI LINUX

oleh Zahwa Amir (2502031)

PENDAHULUAN

Kali Linux adalah sistem operasi berbasis Debian Linux yang dirancang secara khusus untuk pengujian keamanan (penetration testing), audit sistem, dan forensik digital.

Dikembangkan oleh Offensive Security, organisasi pelatihan keamanan siber profesional. Kali Linux digunakan oleh ethical hacker, peneliti keamanan, dan profesional IT untuk menguji keamanan jaringan dan sistem komputer.



SEJARAH

Awalnya Kali Linux dikenal dengan nama BackTrack Linux, dibuat oleh Mati Aharon dan Max Moser pada tahun 2006. BackTrack merupakan sistem operasi berbasis Ubuntu, berisi kumpulan tools untuk uji penetrasi dan keamanan jaringan. Karena kebutuhan sistem yang lebih stabil, pada tahun 2013, proyek ini dikembangkan ulang menjadi Kali Linux dengan basis Debian.

BackTrack dibuat dari gabungan dua distribusi Linux sebelumnya, yaitu Whax dan Auditor Security Collection, yang keduanya sama-sama digunakan untuk pengujian keamanan jaringan (penetration testing).

Tujuan BackTrack adalah menyediakan satu sistem operasi yang berisi semua alat hacking dan forensik digital dalam satu paket.

PERKEMBANGAN VERSI

2013 (Kali Linux 1.0)= Rilis perdana, berbasis Debian 7 (Wheezy)

2015 (Kali Linux 2.0 ("Sana"))= Antarmuka dan sistem diperbarui besar-besaran

2019 (Kali Linux Rolling Release)= Pembaruan bergulir (rolling) seperti Arch Linux

2020 (Mode Non-Root Default)= Demi keamanan, pengguna default bukan root

2022–2025 (Versi terbaru terus dikembangkan)=Dukungan untuk ARM, mobile, cloud, dan WSL (Windows Subsystem for Linux)

FUNGSI UTAMA

- **Penetration Testing**= Melakukan pengujian keamanan sistem dan jaringan untuk menemukan celah atau kelemahan.
- **Security Auditing**= Mengevaluasi dan memeriksa tingkat keamanan infrastruktur IT suatu organisasi.
- **Digital Forensics**= Menganalisis data dan bukti digital setelah terjadinya insiden keamanan.
- **Network Monitoring**= Memantau lalu lintas jaringan untuk mendeteksi aktivitas mencurigakan.
- **Vulnerability Assessment**= Mengidentifikasi dan memverifikasi potensi kerentanan dalam sistem.
- **Wireless Security Testing**= Menguji dan mengamankan jaringan Wi-Fi dari potensi serangan

FITUR UTAMA

- Open Source & Gratis= Bebas digunakan dan dimodifikasi oleh siapa pun.
- Ribuan Tools= Keamanan Lebih dari 600 alat keamanan siap pakai.
- Multi Platform Support= Dapat dijalankan di berbagai perangkat.
- Rolling Release System= Pembaruan terus-menerus tanpa instal ulang.
- Customizable ISO= Dapat dibuat versi khusus sesuai kebutuhan pengguna.
- Live Boot & Persistence Mode= Bisa dijalankan tanpa instalasi.
- Dukungan Multi Bahasa= Termasuk Bahasa Indonesia.
- Keamanan Tinggi & Privilege Management= Sistem keamanan ketat untuk penggunaan profesional.

KELEBIHAN

- **Gratis dan Open Source** Dapat digunakan bebas tanpa lisensi.
- **Lengkap dengan Tools Keamanan** Lebih dari 600 tools profesional sudah tersedia.
- **Komunitas Aktif dan Dokumentasi Lengkap** Dukungan global untuk pengguna baru.
- **Stabil dan Ringan** Dapat berjalan pada spesifikasi perangkat menengah.
- **Dukungan Banyak Platform** Bisa dijalankan di berbagai perangkat dan arsitektur.

KEKURANGAN

- Tidak Ramah Pemula Memerlukan pemahaman sistem Linux dan command line.
- Kurang Cocok untuk Penggunaan Harian Tidak ideal untuk kegiatan seperti mengetik, multimedia, dll.
- Akses Root yang Berisiko Kesalahan perintah dapat menyebabkan kerusakan sistem.
- Aplikasi Umum Terbatas Tidak mendukung aplikasi populer seperti Microsoft Office.
- Potensi Penyalahgunaan Harus digunakan untuk tujuan etis dan legal.

CONTOH PENGGUNAAN

- Pengujian Keamanan Jaringan (Penetration Testing)

Digunakan untuk menguji kekuatan jaringan dan menemukan celah keamanan.

Contoh alat: Nmap, Metasploit, OpenVAS.

- Keamanan Website

Menguji keamanan situs web dari serangan seperti SQL Injection atau XSS.

Contoh alat: Burp Suite, OWASP ZAP, Nikto.

- Forensik Digital

Menganalisis bukti digital setelah terjadi serangan siber.

Contoh alat: Autopsy, Foremost, Volatility.

- Keamanan Wi-Fi

Menguji kekuatan enkripsi dan keamanan jaringan nirkabel.

Contoh alat: Aircrack-ng, Reaver, Kismet.

- Uji Kekuatan Password

Menguji apakah password aman dari serangan brute force.

Contoh alat: John the Ripper, Hydra, Hashcat.

- Pendidikan dan Pelatihan

Digunakan oleh mahasiswa dan profesional untuk belajar ethical hacking dan keamanan siber.

- Audit Keamanan Perusahaan

Perusahaan menggunakan Kali Linux untuk memeriksa keamanan server, sistem, dan aplikasi sebelum digunakan publik.

TERIMA KASIH

